Sense of Security	Authorisation. Jason Edelstein
	Release date. 03 May 2011.

Sense of Security – Security Advisory – SOS-11-005.

Proofpoint Protection Server Cross-Site Scripting Vulnerability.

03 May 2011.

Proofpoint Protection Server Cross-Site Scripting - Security Advisory - SOS-11-005

Release Date.	03-May-2011
Last Update.	-
Vendor Notification Date.	20-Apr-2011
Product.	Proofpoint Protection Server
Platform.	Appliance
Affected versions.	5.5.5 (verified), and possibly others
Severity Rating.	Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch
CVE reference.	Not yet assigned

Details.

The Proofpoint Protection Server offers anti-spam and anti-virus, connection management, email firewall and policy enforcement features.

A Cross-Site Scripting (XSS) vulnerability has been discovered in the Proofpoint Protection Server where input is passed to the query string of process.cgi. This has occurred as a result of the application not properly filtering HTML tags which allows malicious JavaScript to be embedded. When input is incorrectly validated and not properly sanitised and then displayed in a web page, attackers can trick users into viewing the web page and causing malicious code to be executed.

Proof of Concept.

The Cross-Site Scripting vulnerability can be triggered by using the following URL:

https://proofpoint.yyy.com.au:10020/enduser/process.cgi?cmd=release&recipient=xxx@yyy.com.au&msg_id=%28MDYzMjU0NTJkYTQ0OWRhYjJlNWY1MjBhNzc5MDEwODlkZGY5OGIzMTc1MGI=%29&locale=enus&x=580&y=470&displayprogress=t%22%20onmouseover=%22alert%281%29%22%20name=%22frame_display%22%20id=%22frame_display%22%20NORESIZE%20SCROLLING=%22no%22%20/%3E%3C!--

Where:

- proofpoint.yyy.com.au:10020 is the internal FQDN of the Proofpoint appliance (this is the link received in the 'quarantine mail alert' email)

Note: the recipient and msg_id parameters do not need to be valid (exist on Proofpoint) to trigger the vulnerability.

Solution.

The vendor has advised that ‘Patch 1084’ is now available, and should be applied to fix this issue.

Discovered by.

Karan Khosla from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia’s premier application penetration testing firm and trusted IT security advisor to many of the country’s largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-005.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php